Flexible Delivery in Information Security Education

William J. Caelli, Edward P. Dawson, Mark H. Looi

Abstract-- **There is a worldwide shortage of information security specialists. Increased professional training through academic institutions is needed to help fill this demand. In this paper we describe our extensive experience in information security/assurance education over the past twelve years highlighting some of the lessons that we have learned. We describe our current flexible information security education program and discuss future developments in this program.**

Index Terms **Flexible Delivery, Postgraduate Studies, Security Education**

I. Introduction

With the ever increasing dependence of society, nationally and internationally, on an electronic environment there is a need to develop information security processes, services and mechanisms. The information economy is at risk, as was clearly stated by the former USA National Coordinator for Security, Infrastructure Protection and Counter-terrorism, Mr Richard A Clarke. In May 1999[i] he made the following observation: *the conclusion by the Administration is that the nation IS at risk because over the last decade we have made the nation, the economy and national defense dependent upon computer networks. We have designed, ad hoc, a national information infrastructure without any thought of including security.*

In order to manage these mechanisms trained and educated professionals are required. In order to train such professionals centres of such training and education are required. These needs were foreshadowed at the Queensland University of Technology (QUT), over 12 years ago, in Brisbane Australia leading to the creation of the Information Security Research Centre (ISRC) in 1988. The ISRC was set up with a goal for providing research, education, training and consultancy services in information security to meet the needs of both public and private enterprises on a global basis.. The ISRC is currently located within the School of Data Communications, one of the three schools within the Faculty of Information Technology within the University. The ISRC is the research facility within the School of Data Communications and is itself recognised as a "University Centre", capable of supporting cross-discipline education and R&D activities.

The research interests of the ISRC cover most areas of information security. Thus, there are four separate but cooperating research groups within the ISRC, namely Cryptology, Secure Electronic Commerce, Network and Systems Security, and Security Policy/Management and Risk Assessment. The research of the ISRC is supported by its Secure Networks Laboratory. There are 25 staff and 32 research students within the ISRC. Staff members are drawn from the ISRC itself as well as from the School of Data Communications and other Schools within the Faculty.

Over a twelve year period an extensive information security education program has evolved within the School of Data Communications and the ISRC. The current program involves coursework at both the undergraduate and postgraduate level. The postgraduate level subjects are being offered on campus, in major centres in Australia and elsewhere

Manuscript received March 29, 2001.

W. J. Caelli is the Head of the School of Data Communications, Queensland University of Technology (e-mail: w.caelli@qut.edu.au).

E. P. Dawson is the Director of the Information Security Research Centre, Queensland University of Technology (e-mail: e.dawson@qut.edu.au).

M. H. Looi is the Deputy Director (Consultancy and Continuing Education) of the Information Security Research Centre, Queensland University of Technology (e-mail: m.looi@qut.edu.au)

and through distance education on the internet. Students undertake PhD and research Master s postgraduate programs within the ISRC. As well staff of the ISRC have presented short courses on information security to relevant industry and public enterprise sectors. In this paper an overview of our experiences is presented. We highlight some of the lessons that we have learned during this period. A description of our current flexible program is provided as well as future development. Overall the aims of the ISRC and the School of Data Communications in developing and offering this program are concentrated on meeting the spirit of the recent (2000) statement of Technical Committee 11 (TC-11) of the International Federation for Information Processing (IFIP) which carefully considered its response to the worldwide demand for IT security professionals. IFIP's TC-11 passed the following recommendation at its year 2000 meeting in Beijing, China[ii].

"TC-11 requests all member societies of IFIP (International Federation for Information Processing) to urge their relevant government and education bodies to ensure that proper education and certification requirements are set for those people who intend to become IT security professionals and therefore intend to audit the security of IT systems.
In particular, TC-11 recommends that:
a) minimum education and training requirements be set for any such professionals;
b) any such minimum educational and training requirements should reflect similar standards in like professions;
c) such education and training requirements be developed in line with emerging international standards in the area of information security."

There was a clear recognition in this resolution that proper education and training of IT security professionals must be recognised by government worldwide as a necessity, just as it is in other professional disciplines, e.g. Certified Practicing Accountants, Auditors, etc. There was growing concern that private industry, in particular, was looking to limited, short period classes to "upgrade" IT professionals in other areas to meet the needs of information security and assurance in critical information infrastructures. The ISRC program was designed to counter this short-term view of necessary education, and matches closely the recommendations of TC-11.

II. Experience

In this section we shall overview some of our experiences over the last twelve years in developing a flexible information security education program. This includes mainstream information security subjects, a postgraduate research program, a "graduate certificate" in information security and short courses for industry on specific subjects where pertinent.

A. Mainstream

Since 1988 undergraduate and postgraduate subjects in information security have been presented in an academic setting and for academic credit and award. From 1988 to 1996 four subjects were developed namely Data Security, Introduction to Cryptology, Network Security and Advanced Topics in Cryptology.

1) Data Security

This introductory subject provides students with the foundation for information security studies. The subject is presented at both the undergraduate and postgraduate level. Subject matter areas covered include basic concepts in information security and related standards, security management, basic concepts in cryptology (from a *"black box"*

viewpoint) and applications of information security. This is a required subject for all students undertaking major studies in the School of Data Communications. Currently there are over 500 students taking this unit each year.

2) Introduction to Cryptology

This subject provides students with the basic concepts in cryptology. It is presented at both the undergraduate and postgraduate level. Areas of presentation include background mathematics, classic ciphers, symmetric ciphers, public key ciphers, key management and applications of cryptography. Currently there are over 100 students taking this unit each year.

3) Network Security

This subject provides students with a background covering the basic concepts in network security. This subject is presented at the postgraduate level only. Students are required to have previously taken either Data Security or Introduction to Cryptology as well as an introductory subject to basic concepts in data communications and networks. Areas of presentation include risk assessment and management in a network environment, placement of security services and mechanisms in network architectures, layer services and mechanisms using the OSI model as a base, security and the Internet, placement of cryptographic services, IPSec, SSL, SSH, and allied particular examples as required and, finally, topics in critical infrastructure protection (CIP) / information warfare (IW) and concepts of "trusted networks". Currently about forty students take this subject each year.

4) Advanced Topics in Cryptology

This is a highly specialised unit designed for students undertaking postgraduate research in cryptology. This subject is presented at the postgraduate level only. Students are required to have previously taken the subject "Introduction to Cryptology". Areas of presentation include methods for design and analysis of cryptographic algorithms and protocols. Currently about ten students undertake this subject each year.

It should also be noted that information security also finds a place in allied subjects taught within the School of Data Communications, including undergraduate / postgraduate subjects related to "Network Management" and "Network Authentication".

B. Postgraduate Research

Research degrees are offered in information security at the PhD and Master s level. Each student undertakes research within one of the four research groups of the ISRC. Over the last ten years there have been 21 students who have completed PhD programs and 6 students who have completed a Research Master s degree within the ISRC. Currently there are 25 students enrolled in the PhD program and 6 students enrolled in the Research Masters degree program in the ISRC.

C. Graduate Certificate

From 1991 to 1992 a "graduate certificate" in information security was offered in "intensive mode" on the campus of the University. Students attended three concentrated study blocks of two weeks each. Each block consisted of a combination of lectures and workshops. After successfully completing these blocks students were required to complete a major assignment to finish the graduate certificate program. Topics covered all areas of information security with a concentration on case studies.

D. Industrial Short Courses

Several different short courses have been presented by staff of the ISRC to meet the immediate training needs of industry. These short courses have been of one day to two weeks in duration. A brief description of these courses is presented below.

1) Office of the Australian Federal Attorney General

In 1995-1996 a series of five short courses of two or three days duration each were presented to employees of the Australian Government through the Office of Australian Attorney General. Topics included baseline security, introduction to network security, advanced topics in network security, cryptography and risk assessment.

2) Australian Financial Community

In 1995-1996 a two day short course was presented to the Australian Financial Community on the basic concepts in public key cryptography. This program was presented jointly between staff of the ISRC and the company ERACOM Pty Ltd.

3) Korea Telecom

In 1996 a two week short course on cryptology was presented to engineers from Korea Telecom.

4) Motorola

In 1998 a one week short course on cryptology was presented to engineers from Motorola (Australia).

5) Australian Standards

In 2000, short courses of one day duration each were presented to the Australian business community through "Standards Australia", the official standards setting body for the country. Topics for these courses were concentrated in security management and public key infrastructure (PKI).

III. Lessons Learned

In this section we describe some of the lessons that we have learned during the last twelve years in presenting information security courses.

A. Academic Training

The training of an information security specialist should be conducted by an academic institution resulting in formal, recognised qualification as for any other profession. There are now many commercial organisations offering "certificates" in all areas of information technology. We would argue that in relation to the vital area of information security that such training should not be recognised, in general, as being sufficient. This is in agreement with a recent survey from SANS Institution[iii]. An information security specialist requires the professional education and training from qualified staff within a recognised academic institution, in the same manner as that of other professionals such as accountancy, audit, engineering, law or medicine.

Information security involves a rapidly changing technology set against growing and complex legislative instruments. At its simplest level, the activities of an information security professional in any organisation may themselves be the subject of litigation requiring the appearance of that professional in legal proceedings, enquiries by law enforcement and national defense authorities and the like. It is important that professionals in this area are provided with a proper academic training, that covers thoroughly the main concepts. Anything less

than this could be regarded as negligence by management in not providing the necessary education and training of employees / contractors to create and administer the protection schemes necessary for correct levels of information assurance in the enterprise and for appropriate response mechanisms to be applicable should failure occur.

B. Postgraduate Level

The training of an information security specialist should be at the postgraduate level. Maturity and experience are required to undertake such study. In general undergraduates do not satisfy either of these requirements.

As we have described in Section II.A above, in our undergraduate information technology degree at QUT two subjects, namely Data Security and Introduction to Cryptology, are offered. However, it should be noted that these subjects are meant to provide an introduction to basic concepts not to provide the educational background needed by a trained IT security professional.

C. Correct Background

It is important that students undertaking postgraduate training in information security have sufficient background. One area for which it is important to have a knowledgeable and competent background is in basic principals of data communications and networks as well as in operating systems and their interactions with those networks of host and client applications. If students do not have such a background it may be necessary to have available such subjects.

D. Research Centre

Information security is a fast changing discipline. The personnel involved in providing postgraduate education courses need to be researchers at the leading edge of research in the discipline. Also information security covers a wide breadth of material so that these educators should be able to provide background across the many different areas associated with information security arena, from cryptology to network security to security policy and associated legal / audit topics. The ISRC has been structured to provide both the depth and breadth required in information security. We claim that such a research group is needed to provide professional education and training in information security.

E. Choice of Subjects

It is important to select subjects in a postgraduate program in information security which define the overall scope of the discipline. *"Flavour of the month"* topics such as PKI and cryptology for mobile communications should be included as topics within subjects which have a wider scope, not as stand alone subjects.

IV. Current Program

The information security education program at QUT has evolved over the past twelve years. In order to meet the vastly different requirements of both individuals and industry a flexible delivery program has been designed for postgraduate coursework in information security. This program allows for both on-campus enrolment or remote study via the internet.

A. On Campus Program

A postgraduate "Master s Degree by Coursework" at QUT consists of three "semesters" of study with four subjects undertaken in each

semester in the "full-time" study mode. This program caters for both information technology specialist and non-specialist. A non-specialist is required to take background subjects in information technology in the first semester of the program.

All together there are currently six subjects at the postgraduate level offered in information security. These include the four mainstream subjects described in Section 2.1 above as well as two additional units "Topics in Security" and "Access Control" described below. In addition students undertake projects in information security which are equivalent to either one, two or four subjects/units of study.

The student who enters the program as a non-specialist in information technology can undertake the equivalent of eight subjects at most in information security while for the specialist it is possible to undertake all twelve subjects in information security.

In addition there are available postgraduate subjects in various areas of data communications such as network management and network administration. Subjects relevant to the study program may also be chosen from other disciplines, e.g. audit, etc.

1) Topics In Security

This subject consists of individual lectures by specialists on a broad range of topics in information security. This subject is presented at the postgraduate level only. Students who undertake this subject are required to be at least taking another information security subject concurrently. Currently (2001) about fifteen students are taking this subject.

2) Access Control

Access control forms the "front line" in control and management of network based information systems, particularly those deployed on national and international bases. A postgraduate subject was designed to provide this background. This subject focuses on the different types of access control systems possible, formal models for access control, and explores different situations where access control systems are used. Students undertake a small project and a research paper as a part of the assessment. Current enrolments are approximately forty students per year.

3) Data Communications Subjects

One of the main driving forces behind the surge in demand for information security specialists has been the networking of information systems. Thus, many of the issues that information security professionals must deal with are centered around information networks. We run several data communications and networking subjects to ensure that students without the formal networking background can gain the necessary knowledge. Relevant units include Network Administration, Network Management, Internet Applications, Internetworking and Network Programming.

B. Graduate Certificate in Information Security by Remote Education

The Faculty of Information Technology runs a Professional Masters program comprising twelve subjects offered externally using remote delivery means. For the most part, this involves the delivery of the material and interaction with students using the Internet.

As a part of this Professional Masters program, the ISRC offers the "Graduate Certificate in Information Security", as mentioned earlier. The Graduate Certificate consists of four subjects, Data Security (to be renamed Information Assurance

from the 2002 academic year), Introduction to Cryptology, Network Security and Access Control. These four subjects mirror the on-campus program described above. Students also have the option of completing an industry based project instead of one of the coursework subjects. Students can also complete a major project (equivalent to four subjects) in order to upgrade to a Graduate Diploma in Information Security. There are long term plans to offer more subjects as a part of this program, thus allowing a student to complete eight coursework subjects in information security along with a major project, in order to receive the Masters qualification.

V. Future Developments

There are several areas that are planned in order to extend the current program in the near future, as described below. These new subjects have been carefully considered in the light of suggestions and requests from both the private and public sectors.

A. Greater Flexibility

Groups which are seeking to increase rapidly the number of personnel in information security have requested a concentrated on site information security training program leading to a graduate certificate in information security. It is planned to use the same four subjects as presented in the remote education program (see Section IV.B above) for on site presentations. This will involve six hours of class contact per day with two professional education staff. Hence in the future we will offer postgraduate training on campus, at off campus locations and remotely by the internet.

B. Additional Subjects

There are several subjects in information security which we are planned for addition to our existing program of postgraduate study.

1) Computer Forensics

Industry and government have clearly expressed the need for education in the broad area of "computer forensics", i.e. the techniques and principles in involved in the investigation of computer based crime and the collection and presentation of associated evidentiary materials. This means that the information assurance professional of now and of the future must face the prospect of simply appearing in court with the associated problems of admission as an "expert" and the responsibilities that are implied by that recognition in legal proceedings. Techniques of "EDP Audit", computer evidence collection and verification procedures, preparation and presentation of evidence in investigation and court proceedings and the like are all required along with basic understandings of legal matters and policing requirements.

2) Trusted Computing

The adoption of the so-called "Common Criteria" (IS 15408) as an international standard has clearly focussed attention on the basic security "fitness" of commercial IT products and services. These are usually designated as "Commercial-off-the-Shelf (COTS)" systems and they are being incorporated into mission, corporate and nationally critical information infrastructures. With the adoption of such schemes a PKI on a global basis for the provision of at least authentication services in electronic commerce systems highlights the need for understanding of this vital topic. As much as any safety and security standards sets exist in other industries, e.g. the motor vehicle, airline and other industries, the "Common Criteria" will provide a base "check list" for the information security professional to determine any "add-in" security sub-

systems that may be needed in an overall information system. It may also provide a base for "pressure" to be applied, where needed, on manufacturers to meet basic safety and security needs in interconnected systems, particularly at the basic hardware and operating system levels upon which all integrated electronic commerce systems will be built.

C. *Increase "Hands on" Experience*

A challenge facing educators of information security programs is that of increasing the amount of practical "hands on" experience that can be provided to the students. Information security hands on sessions generally mean that the students must have full "administrator" and like access to the laboratory computers and network systems, e.g. "firewalls", routers, host server systems, etc. This can prove difficult to manage and costly.

However, students are demanding this additional hands on experience. Thus, we (and other information security educators) must develop suitable techniques and mechanisms for providing this to a large number of students.

Providing such an experience to off-campus students will prove to be even more difficult. We are currently exploring a network architecture that permits students to manage and administer a number of test and laboratory networked computers, network components, firewalls and the like with differing network configurations remotely. A separate control network will be connected to the Internet using secure authentication technologies to allow the students to control the experimental configuration and to monitor the results of their configuration changes and associated experiments. It is hoped that such a system will be trialed in the July 2001 semester at QUT.

The question of appropriate simulators has been considered and such systems offer promise if constructed in an innovative and flexible manner. However, development of such systems and the associated "courseware" is expensive and usually beyond the capability of publicly funded tertiary education institutions such as QUT. In order to assist with future development in this direction extra funds from government and/or private industry may be required.

VI. Conclusions

Highly educated and trained professionals in information security are required to assist with the protection of critical information infrastructures. To meet the diverse requirements of people wanting to undertake training for such a profession we have designed a highly flexible program. There are no "short cuts" to the provision of the levels of education needed to enable the proper management of global electronic commerce systems. Indeed, any move to "quick", industry based courses could be counterproductive in that both private and public enterprises could become dependent upon under-educated personnel. This easily gives a false sense of security, particularly if law enforcement and/or national security matters are involved. Indeed, this matter of under training of IT security "managers" has been identified in a recent SANS Institute survey as being THE major problem in relation to information systems protection. The SANS survey clearly stated its findings, under a major heading, as follows:

THE SEVEN WORST SECURITY MISTAKES SENIOR EXECUTIVES MAKE

- *Assigning untrained people to maintain security and providing neither the training*

nor the time to make it possible to learn and do the job.

- *Failing to understand the relationship of information security to the business problem — they understand physical security but do not see the consequences of poor information security.*

Management needs to see that investment in proper education and training of professionals in this area is a mandatory requirement of "due diligence" in corporate and government management.

As was shown in the mid-1960s with the car industry, it may be that Government legislation may be needed to compel public/private sector management to invest the necessary money needed to provide the levels of educated and trained professionals required to protect the single most valuable asset of any enterprise, its information. After all, this is clearly the case in all other forms of law enforcement and national defense, let alone in normal safety and protection of other enterprise assets.

REFERENCES

[i] Clarke, Richare A. President s Initiative in Building a Natural Cybercorps Program , NCISSE 1999 Conference, New York, USA (May 1999).

[ii] Minutes of the Meeting of IFIP Technical Committee 11, Beijing, China. (August 2000).

[iii] SANS Institute, 2000.